JOURNAL OF NUMBER THEORY 28, 283–287 (1988)

Cyclotomic Polynomials and Units in Cyclotomic Number Fields

MICHAEL KAMINSKI

Department of Computer Science,
Technion - Israel Institute of Technology, Haifa 32000, Israel

Communicated by O. Taussky Todd

Received February 10, 1987; revised February 24, 1987

Let $P(x) \neq x$ be a monic irreducible polynomial with integer coefficients such that for infinitely many n, $P(e^{2\pi i/n})$ is a unit in the ring of algebraic integers $Z[e^{2\pi i/n}]$. It is shown that $P(x)$ is a cyclotomic polynomial. © 1988 Academic Press, Inc.

Let ω_n denote an nth primitive root of unity, $\omega_n = e^{2\pi i/n}$, say, and let $\Phi_n(x)$ denote the nth cyclotomic polynomial, i.e., the minimal monic polynomial of ω_n. $\Phi_n(x)$ has integer coefficients, and $\deg \Phi_n(x) = \phi(n)$, where ϕ is Euler's function. It is known that if the ratio of two positive integers n_1 and n_2 is not a non-zero power of a prime number, then the resultant $\rho(\Phi_{n_1}(x), \Phi_{n_2}(x)) = \pm 1$, cf. [1]. Below we prove the following kind of a converse of this property of cyclotomic polynomials.

THEOREM 1. *Let $P(x) \neq x$ be a monic irreducible polynomial with integer coefficients such that its resultant with infinitely many cyclotomic polynomials is ± 1. Then $P(x)$ is a cyclotomic polynomial.*

The resultant of two polynomials is equal to ± 1 if and only if the polynomials generate comaximal ideals in $Z[x]$, cf. [3, p. 136]. Hence Theorem 1 is equivalent to each of the following.

THEOREM 2. *Let $P(x) \neq x$ be a monic irreducible polynomial with integer coefficients such that for infinitely many n, $P(\omega_n)$ is a unit in the ring of algebraic integers $Z[\omega_n]$. Then $P(x)$ is a cyclotomic polynomial.*

THEOREM 3. *Let $\alpha \neq 0$ be an algebraic integer such that for infinitely many n, $\Phi_n(\alpha)$ is a unit in the ring of algebraic integers $Z[\alpha]$. Then α is a root of 1.*

It is well known that if l is an integer prime to n, then $1 - \omega_l^n$ is a unit in $Z[\omega_l]$, cf. [4, p. 72]. The corollary to Theorem 3 below is tightly connected to the above property of roots of 1.

0022-314X/88 $3.00

COROLLARY. *Let $\alpha \neq 0$ be an algebraic integer such that for infinitely many n, $1 - \alpha^n$ is a unit in the ring of algebraic integers $Z[\alpha]$. Then α is a root of 1.*

The proof of Theorem 1 is based on the following theorem of A. Baker [2].

Let $\alpha_1, ..., \alpha_m$ be non-zero algebraic numbers with degrees at most d and let the heights of $\alpha_1, ..., \alpha_{m-1}$ and α_m be at most A' and A ($\geqslant 2$), respectively. Then for some effectively computable number $C > 0$ depending only on m, d, and A', the inequalities

$$0 < |b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m| < C^{-\log A \log B}$$

have no solution in rational integers $b_1, ..., b_m$ with absolute values at most B ($\geqslant 2$).

For applying the above theorem we need some preliminaries.

PROPOSITION 1. *If $|\alpha| > 1$, then $|\Phi_n(\alpha)| > e^{-1/(|\alpha|-1)} |\alpha|^{\phi(n)}$.*

Proof. Since $\Phi_n(x) = \prod_{k|n} (x^{n/k} - 1)^{\mu(k)}$, where $\mu(k)$ is the Möbius function, cf. [3, p. 207],

$$\left| \frac{\Phi_n(\alpha)}{\alpha^{\phi(n)}} \right| = \left| \prod_{k|n} \left(1 - \frac{1}{\alpha^{n/k}}\right)^{\mu(k)} \right| > \prod_{k=1}^{\infty} \left(1 - \frac{1}{|\alpha|^k}\right).$$

Taking the logarithms of both sides, using an estimation

$$\ln \prod_{k=1}^{\infty} \left(1 - \frac{1}{|\alpha|^k}\right) = \sum_{k=1}^{\infty} \ln \left(1 - \frac{1}{|\alpha|^k}\right) > - \sum_{k=1}^{\infty} \frac{1}{|\alpha|^k} = \frac{-1}{|\alpha| - 1},$$

and exponentiating back, we obtain the desired result. ∎

PROPOSITION 2. *If $|\alpha| \leqslant 1$, then $|\Phi_i(\alpha)| \leqslant 2^{\phi(n)}$.*

Proof. Since

$$\Phi_n(x) = \prod_{\substack{(i,n)=1 \\ i<n}} (x - \omega_n^i),$$

$$|\Phi_n(\alpha)| = \left| \prod_{\substack{(i,n)=1 \\ i<n}} (\alpha - \omega_n^i) \right| \leqslant \prod_{\substack{(i,n)=1 \\ i<n}} (|\alpha| + 1) \leqslant 2^{\phi(n)}. \quad ∎$$

PROPOSITION 3. *Let $m = p_1 \cdots p_s$ be a square-free integer with its prime factorization. Then $x^m - 1 = \Phi_m(x) \prod_{i=0}^{s-1} \Phi_{p_1 \cdots p_i}(x^{p_{i+2} \cdots p_{s-1} p_s})$.*

Proof. The proof goes by induction on s. If $s=1$, then $m=p_1$, and $x^{p_1}-1=\Phi_{p_1}(x)\,\Phi_1(x)$. For the induction step assume that the proposition holds for $s-1$, and prove it for s. Let $y=x^{p_s}$, and let $m'=m/p_s$. Then $x^m=y^{m'}$, and, by the induction hypothesis, $y^{m'}-1=\Phi_{p_1\cdots p_{s-1}}(y)\prod_{i=0}^{s-2}\Phi_{p_1\cdots p_i}(y^{p_{i+2}\cdots p_{s-1}p_{s-1}})$. Substituting x^{p_s} for y in the above identity results in $x^m-1=\Phi_{p_1\cdots p_{s-1}}(x^{p_s})\prod_{i=0}^{s-2}\Phi_{p_1\cdots p_i}(x^{p_{i+2}\cdots p_{s-1}p_s})$. Since $\Phi_m(x)\,\Phi_{m'}(x)=\Phi_{m'}(x^{p_s})$, cf. [3, p. 206], the proof follows. ∎

PROPOSITION 4. *Let $n=p_1^{r_1}\cdots p_s^{r_s}$ be a positive integer with its prime factorization. If $|\alpha|\leqslant 1$, then $|\alpha^n-1|<|\Phi_n(\alpha)|\,2^{\sum_{i=0}^{s-1}\phi(\prod_{j=1}^{i}p_j)}$.*

Proof. For $m=p_1\cdots p_s$, $n'=n/m=p_1^{r_1-1}\cdots p_s^{r_s-1}$, and $\beta=\alpha^{n'}$, by Proposition 3, we have

$$|\alpha^n-1|=|\beta^m-1|=\Phi_m(\beta)\prod_{i=0}^{s-1}\Phi_{p_1\cdots p_i}(\beta^{p_{i+2}\cdots p_s}).$$

$|\alpha|\leqslant 1$, implies $|\beta|\leqslant 1$. Hence for all $i\leqslant s-1$ we have $|\beta^{p_{i+2}\cdots p_s}|\leqslant 1$, and, by Proposition 2, $|\Phi_{p_1\cdots p_i}(\beta^{p_{i+2}\cdots p_s})|\leqslant 2^{\phi(\prod_{j=1}^{i}p_j)}$. Since $\Phi_n(x)=\Phi_{p_1\cdots p_s}(x^{p_1^{r_1-1}\cdots p_s^{r_s-1}})$, cf. [3, p. 206], substituting $\Phi_n(\alpha)$ for $\Phi_m(\beta)$, and $2^{\phi(\prod_{j=1}^{i}p_j)}$ for $|\Phi_{p_1\cdots p_i}(\beta^{p_{i+2}\cdots p_s})|$, $i=1,2,\ldots,s-1$, in the last identity completes the proof. ∎

Let $n=p_1^{r_1}\cdots p_s^{r_s}$ be a positive integer with its prime factorization such that $p_1<p_2<\cdots<p_s$. Define $\theta(n)$ by $\theta(n)=\sum_{i=0}^{s-1}\phi(\prod_{j=1}^{i}p_j)$.

PROPOSITION 5.

$$\lim_{n\to\infty}\frac{\theta(n)}{\phi(n)}=0.$$

Proof. It suffices to show that for large values of n we have, say, $\theta(n)/\phi(n)\leqslant 2(\log\log n)^2/\log n$.[1] By definitions of $\theta(n)$ and $\phi(n)$ we have

$$\frac{\theta(n)}{\phi(n)}<\frac{\sum_{i=0}^{s-1}\prod_{j=1}^{i}(p_i-1)}{\prod_{j=1}^{s}(p_i-1)}\frac{1}{p_1^{r_1-1}\cdots p_s^{r_s-1}}$$

$$=\frac{\sum_{i=0}^{s-1}\prod_{j=i+1}^{s-1}(p_i-1)^{-1}}{p_s-1}\frac{1}{p_1^{r_1-1}\cdots p_s^{r_s-1}}<\frac{2}{p_s-1}\frac{1}{p_1^{r_1-1}\cdots p_s^{r_s-1}},$$

where the last inequality follows from the fact that $p_1, p_2, \ldots, p_s$ are distinct prime numbers.

[1] By a more involved argument one can show that $\theta(n)/\phi(n)$ does not exceed $(1+2/\log n)/\log n$.

Now, if $p_s > \log n/(\log\log n)^2$, then, definitely, $\theta(n)/\phi(n) \leqslant 2(\log\log n)^2/\log n$. Otherwise, $s < \log n/(\log\log n)^2$, and we have

$$\frac{\theta(n)}{\phi(n)} < \frac{2}{p_s - 1}\frac{1}{p_1^{r_1-1}\cdots p_s^{r_s-1}} < \frac{2p_1 p_2 \cdots p_s}{n}$$
$$\leqslant \frac{2p_s^s}{n} < \frac{2(\log n)^{\log n/(\log\log n)^2}}{n} = \frac{2n^{1/\log\log n}}{n}.$$

For large values of n the last expression does not exceed $(\log\log n)^2/\log n$. ∎

Proof of Theorem 1. Assume, by contradiction, that $P(x)$ is not cyclotomic. We break the proof into several steps.

(1) *There exist* $C_1 < 1$ *and a root of* $P(x)$, λ, *such that for infinitely many* n, $|\Phi_n(\lambda)| \leqslant C_1^{\phi(n)}$.

Let $\lambda_1, \lambda_2, \ldots, \lambda_l$ be all the roots of $P(x)$. Since $P(x)$ is non-cyclotomic there exists an i such that $|\lambda_i| \neq 1$, cf. [4, p. 105]. Therefore for some j we have $|\lambda_j| > 1$, because $\prod_{i=1}^{l} \lambda_i$ is an integer. Since $\rho(\Phi_n(x), P(x)) = \pm 1 = \prod_{i=1}^{l} \Phi_n(\lambda_i)$, and $|\Phi_n(\lambda_j)| > e^{-1/(|\lambda_j|-1)}|\lambda_j|^{\phi(n)}$, for some root of $P(x)$, λ and for infinitely many n we have

$$|\Phi_n(\lambda)| < (e^{1/(|\alpha|-1)}|\lambda_j|^{-\phi(n)})^{1/(l-1)} < C_1^{\phi(n)},$$

where $1/|\lambda_j|^{1/(l-1)} < C_1 < 1$. ∎

(2) *Let* λ *be as in* (1), *There exists a constant* $C_2 < 1$ *such that for infinitely many* n, $|\lambda^n - 1| \leqslant C_2^{\phi(n)}$.

From (1) and Proposition 4 for infinitely many n we have $|\lambda^n - 1| < C_1^{\phi(n)} 2^{\theta(n)}$. Since, by Proposition 5, $\theta(n) = o(\phi(n))$, (2) holds with C_2 satisfying $C_1 < C_2 < 1$. ∎

(3) *Let* λ *be as in* (1). *There exists a constant* $C_3 < 1$ *such that for infinitely many* n, *there exists a* $|b| \leqslant n$, *satisfying* $|2K\pi i - b\log\lambda| < C_3^{\phi(n)}$.

It follows from (2) that $|\lambda| = 1$. Then for any C_3 such that $C_2 < C_3 < 1$, and for a sufficiently large n satisfying (2), (3) holds with $b = n$. ∎

Now, since $\phi(n) > n^{1-\delta}$, (3) contradicts Baker's theorem with $m = 2$, $\alpha_1 = 1$, $\alpha_2 = \lambda$, $b_1 = 1$, $b_2 = b$, and $B = n$. This completes the proof of Theorem 1. ∎

Remark. Actually, something stronger than Theorem 1 has been shown. Namely, *given a noncyclotomic monic irreducible polynomial* $P(x) \neq x$, *and* $C > 1$, *there exists an effectively computable constant* N *such that if* $n > N$, *then* $|\rho(P(x), \Phi_n(x))| > C^{\phi(n)}$.

REFERENCES

1. T. M. APOSTOL, Resultants of cyclotomic polynomials, *Proc. Amer. Math. Soc.* **24** (1970), 457–462.
2. A. BAKER, A sharpening of the bounds for linear forms in logarithms, *Acta Arith.* **XXI** (1972), 117–129.
3. S. LANG, "Algebra," Addison–Wesley, Reading, MA, 1965.
4. S. LANG, "Algebraic Number Theory," Addison–Wesley, Reading, MA, 1970.